PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF APPEALS AND INTERFERENCES

Application No.	:	10/518,545
Confirmation No.	:	9542
Applicant	:	Eugenio Ferreira Da Silva Neto
Filed	:	03 Jan. 2005
Title	:	Method providing protection from unauthorized access to a field device used in process automation technology
TC/A.U.	:	2431
Examiner	:	B. F. Wright
Docket No.	:	DASI3002/FJD
Customer No.	:	23364

BRIEF ON APPEAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA. 22202-3514

Sir:

INTRODUCTORY COMMENTS

Pursuant to the provisions of 37 CFR 41.37, submitted herewith is Applicant/Appellant's Brief on Appeal along with the required fee. The period for response has been extended to expire on June 2, 2010, by filing herewith a Petition for a One Month Extension of Time and payment of the required fee.

Any additional fees necessary for this appeal may be charged to the undersigned's Deposit Account No. 02-0200.

REAL PARTY IN INTEREST
(37 CFR 41.37(c)(1)(i)

The real party in interest is Applicant/Appellant's assignee Endress + Hauser Process Solutions AG. The assignment was recorded on February 8, 2006, at Reel 017246 and Frame 0548.

RELATED APPEALS AND INTERFERENCES
(37 CFR 41.37(c)(1)(ii)

There are no related appeals or interferences with respect to the invention defined in this application.

STATUS OF CLAIMS
(37 CFR 41.37(c)(1)(iii))

Claims 1 - 11 have been cancelled.

Claims 12 - 22 are pending in this application.

Claims 12 - 22 have been finally rejected and are therefore the subject of this appeal.

STATUS OF AMENDMENTS
(37 CFR 41.37(c)(1)(iv))

No amendment was filed after issuance of the Office Action of December 2, 2009.

SUMMARY OF CLAIMED SUBJECT MATTER
(37 CFR 41.37 (c)(1)(v))
(References are to page and line of the specification)

The method being considered on this appeal relates to a method for providing protection from unauthorized access to a field device used in process automation technology (pg 1, lines 3 - 5), and more particularly to such a method which prevents unauthorized changing of the configuration of the field device (pg. 3, lines 13 and 14).

An essential ideaq of the invention is the storing of a security program in the field device itself. The security program performs an authorization examination, and in this way, a manipulation of the field device without authorization can be prevented (pg 3, lines 18 - 21).

Eleven claims define the invention, and these claims have been finally rejected. Of the eleven claims, claim 12 is in independent form, while claims 13 - l22 are in dependent form, all dependent from claim 12. Claim 12, in annotated form, is reproduced below.

12. A method for providing protection from unauthorized access to a field device in process automation technology, whereby the field device is connected over a data bus with a remote control unit (Fig. 1 and pg. 3, lines 27 - 29), the field device comprises at least one function block with defined communications interfaces (pg. 4, lines 18 - 24), whereby the set parameters of the function block and the field device determine the functionality of the field device and allow the execution of complicated control procedures while interacting with other field devices and allow the execution of complicated control procedures while interacting with other field devices connected to the data bus (pg 4, lines 19 - 28), the method comprising the steps of:

storing in the field device or in the function block a security program (pg 5, lines 1 and 2);

performing an authorization examination in the case of accessing the parameters of the function block or the field device over the data bus (pg 5, lines2 - 4); and

permitting a change in the parameters of the function block or the field device or a replacement of the function block only in the case when the authorization is available (pg 5, lines 4 - 9)

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
(37 CFR 41.37(c)(1)(vi))

There are two final rejections presented, these are:

(1) claims 12 - 15 and 17 -22 are finally rejected under 35 USC 103(a) over Gillen in view of Crater et al and Galasso; and

(2) claim 16 is finally rejected under 35 USC 103(a) over Gillen and Crater et al in view of Galasso and Moyer.

These rejections are respectfully traversed.

ARGUMENT

(1)

For the record, it is noted that Gillen teaches that the programmable field measuring instrument encompasses an "internal" control unit which serves for executing a control program. Connected to this "internal" control unit is a non-volatile software program memory. Furthermore, there is an interface as a connector terminal which is connected in a manner to be released to a software protection device. The protection device, a hardware component, comprises a connector mating element with an integrated electronic component which allows authorization examination by the control unit. The integrated electronic component has a micro-controller and should prevent an unauthorized access to the non-volatile software program memory. It was emphasized that Gillen *does not* teach a field device connected over a data bus with a remote control unit with the field device comprising at least one function block with defined communication interfaces.

To this distinction the examiner refers us to paragraph 27 of Gillen and suggests that the teaching in this paragraph "describes the element of remote control of a field device containing software logic....via bus interface."

There is an assumption here that the "control center" disclosed in paragraph 27 is a "remote " control center. This is not necessarily the case.. In fact, it is unlikely the case because of the reliance to Siemens ASIC (Application Specific Integrated Circuit) which are note used for remote applications. The examiner is guessing, and that is not permitted under 35 USC 103.

-4-

For the record, it was also noted that Gillen ***does not*** teach that the set of parameters of the function block and the field device determine the functionality of the field device and allow the execution of complicated control procedures while interacting with other field devices connected to the data bus.

To this distinction, the examiner refers us to paragraph 28 of Gillen and suggests that "applicant's parameters" and "Gillan's variants" are equivalent. Not so. The set parameters must be of the field device ***and*** the function block. It does not appear that the variants can meet this requirement.

Claim 12 defines three steps and not just structure. Gillen does not disclose these steps, and the combination of Gillen with Crater et al and also Galasso also falls short of the claimed invention. Crater et al refers to an integrated control system which comprises one or more controllers each equipped to perform a control function and to gather data relevant to the control function. Each controller contains computer storage means, such as computer memory, for storing the relevant data and instructions, associated with the data, for causing a remote computer to generate a visual display incorporating the data in a predetermined format; and a communication module for establishing contact and facilitating data interchange with the remote computer. Ed How does this teaching assist the person skilled in the art to reach the present invention of claim 12 when this teaching is combined with that of Gillen and Crater et al? It is not readily apparent that their combination is sufficient to reach claim 12.

(2)

Claim 16 depends from claim 12 and further defines the security key. Even if the 128-bit code is taught by the references, they do not, it is respectfully submitted teach the steps of claim 12 as noted above.

The art cited in this prosecution is no doubt analogous. But that is not enough under 35 USC 103. There must be a suggestion that compels the combination found in the references themselves. See, ***In re Gordon***, 221 USPQ 1125 (Fed. Cir. 1984).

This compelling suggestion is missing, and without it, obviousness does not lie.

CONCLUSION

In view of the above, it is respectfully submitted that claims 12 - 22 should be allowed over the references of record and those applied.

Respectfully submitted

BACON & THOMAS, PLLC

Date: June 2, 2010

Félix J. D'Ambrosio
Reg. No. 25,721

BACON & THOMAS, PLLC
625 Slaters Lane, 4th Floor
Alexandria, VA 22314
Tel: (703) 683-0500
Fax: (703) 683-1080
S:\Producer\fjd\CLIENTS\Endress+Hauser Holding GmbH\DASI3002 - PS0014\Brief on Appeal.wpd

Claims 1 - 11 (Cancelled).

12. A method for providing protection from unauthorized access to a field device in process automation technology, whereby the field device is connected over a data bus with a remote control unit, the field device comprises at least one function block with defined communications interfaces, whereby the set parameters of the function block [[an]] and the field device determine the functionality of the field device and allow the execution of complicated control procedures while interacting with other field devices and allow the execution of complicated control procedures while interacting with other field devices connected to the data bus, the method comprising the steps of:

storing in the field device or in the function block a security program;

performing an authorization examination in the case of accessing the parameters of the function block or the field device over the data bus; and

permitting a change in the parameters of the function block or the field device or a replacement of the function block only in the case when the authorization is available.

13. The method as claimed in claim 12, wherein:

the security program is part of a function block.

14. The method as claimed in claim 12, wherein:

the security program is part of firmware stored in the field device.

15. The method as claimed in claim 12, wherein:

the security program includes a security key, which is stored in the field device during configuration of the field device.

16. The method as claimed in claim 12, wherein:

the security key is an at least 128-bit code.

17. The method as claimed in claim 12, wherein:

the security key is created during installation of the field device.

18. The method as claimed in claim 12, wherein:

the security key is provided by the field device.

19. The method as claimed in claim 12, wherein:

the security key is regularly renewed.

20. The method as claimed in claim 12, wherein:

the security key is renewed hourly.

21. The method as claimed in claim 12, wherein:

the security key is stored only in the field device.

22. The method as claimed in claim 12, wherein:

the field devices are sensors, actuators, controllers, PLCs or gateways.

EVIDENCE APPENDIX

There is no evidence being relied upon which was submitted pursuant to 37 CFR 1.130, 1.131 or 1.132.

RELATED PROCEEDINGS APPENDIX

There is no related proceeding being relied upon.